Class Action Litigation Report®

March 27, 2009

Privacy

Companies Face New Twist (and Class Suits) Over Breach of Duty to Protect Data

Although corporations surely reap benefits from the ease and accessibility of electronically stored information, that information poses security risks: Data breaches are increasingly common, and the standards for defining a corporation's duty of care are still evolving.

The standard of care in negligence actions—reasonable care under all the circumstances given the foreseeable risk of harm—takes a twist with data security in large part because there are no clear definitions of what a corporation must do to implement security controls that are "reasonable" or "appropriate." Is encryption enough? Or should you place restrictions on laptop use and information dissemination?

As data breaches become more commonplace, what "reasonable" looks like is becoming more developed. According to two privacy and data security lawyers who spoke with BNA March 3, the development of the "reasonable" standard is moving away from a checklist approach and toward a more process-driven inquiry. The standard of care on which corporations should be leaning requires a more holistic view of the larger data security process. The process, not the specific tools, are where companies should look with respect to protecting data, the lawyers said.

"What we're seeing today is that the standard for data security compliance is becoming focused on a process, rather than on particular controls," said Thomas Smedinghoff, a partner at Wildman Harrold, Chicago.

A process is necessarily objective. It asks what a corporation did and what it should have done, what precautions were available and whether they were enough. It goes beyond the proscriptions of a law and targets the heart of the security framework.

"What is reasonable isn't simply about what a corporation has. Under the evolving process-oriented standard, corporations need to figure out the risks they face, then address those specifically, with the appropriate tools and precautions," Smedinghoff said.

Still, data breach plaintiffs are looking for a way to nail down the negligence standard in order to hold corporations liable when data goes missing or is inappropriately used.

A struggle in these cases is that there is no consensus, even in the existing framework, for what is reasonable, according to **Lisa Sotto, a partner at Hunton & Williams, New York**. It is clear that reasonability is required, but it is not consistently defined.

"There are many different measurements for what makes a corporation's actions appropriate, and there is a lot to look to in creating a standard of care," she said.

Baristas Have Class

A class of Starbucks employees took one approach Feb. 19 when they used guidance issued from both the Federal Trade Commission and the Washington attorney general to create a standard of care that, they said in a complaint, would make Starbucks liable in negligence when an unencrypted laptop containing the personal information of hundreds of employees was lost (Krottner v. Starbucks Corp., W.D. Wash., No. C09-0216, 2/19/09) (10 CLASS 161, 2/27/09).

The FTC's report, "Protecting Personal Information: A Guide for Businesses," offers five "key principles" for corporations to keep in mind with respect to the storage and handling of sensitive information and offers suggested best practices. The Washington attorney general offers similar guidance in its "Consumer Privacy and Data Protection Report."

"Starbucks failed to maintain a number of reasonable security procedures and practices designed to protect the PII [personally identifiable information] of Plaintiff and the Class," the complaint said, and listed among Starbucks' alleged failings standards pulled from both the FTC and AG guides:

- encrypting any sensitive data contained on a laptop;
- refraining from storing sensitive PII on a laptop;
- requiring employees to store laptops in a secure place; and
- allowing laptop users to access sensitive information but not to store the information on their laptops.

These requirements are valid, certainly; but they may not themselves be a binding standard.

In addition to the FTC best practices and state-specific guidances, the Health Insurance Portability and Accountability Act requires protection of health data. The Gramm-Leach-Bliley Act does the same in the financial sector. For government agencies, the Federal Information Security Management Act controls.

Massachusetts recently passed a detailed law requiring businesses to implement written information security programs, and New Jersey has proposed something similar. At least nine other states have data protection laws.

"Taking the view from 50,000 feet, all of these laws and standards say the same thing: You have to provide reasonable and appropriate safeguards," Smedinghoff said.

Defining that which is "reasonable" or "appropriate" is still very much an open question, he said, and is the backdrop for the evolution toward a more fluid process standard. A corporation that adopts a process approach, rather than focusing on facial compliance with any one of the differing laws and regulations, may have a better chance of meeting with success when proving that what it did was reasonable.

Guidance Coming

And the applicable standards themselves may be moving toward a more process-oriented inquiry as well, Sotto said.

The recently passed economic stimulus bill, H.R. 1 (The American Recovery and Reinvestment Act of 2009), requires, at § 13402(h)(2), the Department of Health and Human Services to develop annual standards for protecting sensitive data.

Under the bill:

[T]he Secretary shall, after consultation with stakeholders, issue (and annually update) guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, including the use of standards developed under section 3002(b)(2)(B)(vi) of the Public Health Service Act, as added by section 13101 of this Act.

"This is really something to watch. This is a Congressional mandate to an agency that requires a flexible approach to standards-setting," Sotto said.

Annual updates will ensure that the guidance reflects current technology and relevant best practices, and its focus on methodologies seems consistent with the movement away from strict requirements, Sotto said. The result is likely to be much more flexible than a law and should leave room for a wider consideration of a corporation's larger security process, she said.

The guidance will only be binding on the health sector, but Sotto said she would not be surprised if it became "a benchmark standard for all data breaches going forward."